

10/53494, 5975

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

Rec'd PCT/PTO 16 MAY 2005

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
1 juillet 2004 (01.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/055741 A2

- (51) Classification internationale des brevets⁷ : G07F (72) Inventeur; et
(21) Numéro de la demande internationale : PCT/FR2003/003696 (75) Inventeur/Déposant (pour US seulement) : PANGAUD, Nicolas [FR/FR]; Les Vergers des Belles Terres, 481, route de Nice, F-06560 Valbonne (FR).
(22) Date de dépôt international : 12 décembre 2003 (12.12.2003) (74) Mandataire : MACQUET, Christophe; Murgitroyd & Company, Immeuble Atlantis, 55, allée Pierre Ziller, F-06560 Valbonne Sophia Antipolis (FR).
(25) Langue de dépôt : français
(26) Langue de publication : français (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
(30) Données relatives à la priorité : 0215740 12 décembre 2002 (12.12.2002) FR
(71) Déposant (pour tous les États désignés sauf US) : ASK S.A. [FR/FR]; Les Bouillides, 15, Traverse des Brucs, Sophia Antipolis, F-06560 Valbonne (FR).

[Suite sur la page suivante]

(54) Title: SECURE METHOD FOR MODIFYING DATA RECORDED IN A MEMORY CARD

(54) Titre : PROCÉDÉ SÉCURISÉ DE MODIFICATION DE DONNÉES ENREGISTRÉES DANS UNE CARTE À MÉMOIRE

A. ADRESSE	B SEIZE BITS PAR MOT
0	NUMERO DE SERIE C
1	
2	
3	
4	
5	ZONE 1 D.
6	
7	
8	
9	
10	ZONE 2 E
11	
12	
13	
14	
15	F. COMPTEUR ETAGE A G COMPTEUR ETAGE B
16	
17	ZONE 3 H
18	
19	
20	
21	
22	ZONE 4 I.
23	
24	
25	
26	
27	
28	
29	
30	
31	

A...ADDRESS
B...SIXTEEN BITS PER WORD
C...SERIAL NUMBER
D...ZONE 1
E...ZONE 2
F...STAGE A COUNTER
G...STAGE B COUNTER
H...ZONE 3
I...ZONE 4

(57) Abstract: The invention concerns a method for modifying data in a card transaction system comprising a memory card and a reader adapted to read the card, the card including a non-volatile, erasable and rewriteable memory containing at least one location for recording a data value related to the transactions performed by the card. Each transaction causes the data value to be modified, the latter being monotone in time. Upon each transaction, a data value writing operation writes the new data value (Y) in a first location (B) between two predefined locations of the memory forming a counter, the writing operation erasing the previous data value recorded in the second location (A) such that at the end of the writing operation correctly performed the first location contains the new value while the second location contains the value zero.

(57) Abrégé : Procédé de modification des données dans un système de transaction par carte comprenant une carte à mémoire et un lecteur apte à lire la carte, la carte comprenant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par la carte. Chaque transaction entraîne la modification de la valeur de données, cette dernière étant une fonction monotone dans le temps. A chaque transaction, une opération d'écriture de la valeur de données effectue l'écriture de la nouvelle valeur de données (Y) dans un premier emplacement (B) parmi deux emplacements prédéfinis de la mémoire formant un compteur, l'opération d'écriture effectuant l'effacement de l'ancienne valeur de données enregistrée dans le deuxième emplacement (A) de sorte qu'à la fin de l'opération d'écriture effectuée correctement le premier emplacement contient la nouvelle valeur de donnée alors que le deuxième emplacement contient la valeur zéro.

WO 2004/055741 A2



(84) États désignés (*régional*) : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

**Procédé sécurisé de modification de données enregistrées
dans une carte à mémoire**

5 Domaine technique

La présente invention concerne les systèmes dans lesquels une partie des enregistrements de données mémorisés dans une carte à mémoire est modifiée lors d'une transaction effectuée avec un lecteur de la carte et
10 concerne plus particulièrement un procédé sécurisé de modification de données enregistrées dans une carte à mémoire lors d'une transaction avec un lecteur.

Etat de la technique

15 Les cartes à mémoire encore appelées cartes à puce sont de plus en plus utilisées comme support de données associées aux titulaires des cartes. Parmi ces cartes, les cartes sans contact pour lesquelles l'échange d'informations se fait par couplage électromagnétique sans
20 contact entre une antenne logée dans la carte et un lecteur associé ont été développées comme cartes d'accès à des zones d'accès contrôlé, ou comme porte-monnaie électroniques.

D'une manière générale, les cartes à mémoire
25 utilisent des mémoires non volatiles, effaçables et ré-inscriptibles du type EEPROM ou flash EPROM, de sorte que les données restent inscrites dans la mémoire même lorsque cette dernière est hors tension. Elles permettent en outre une mise à jour des données enregistrées par effacement
30 d'un ou plusieurs emplacements de mémoire et écriture de nouvelles données.

Il peut arriver que, lors d'une transaction, la mémoire soit corrompue en raison d'une interruption accidentelle de l'alimentation électrique due généralement
35 à un "arrachement" de la carte, c'est à dire un retrait de celle-ci avant la fin du traitement, qui entraîne la perte des données antérieures sans enregistrement de nouvelles

données. Ce risque est particulièrement élevé avec les cartes du type sans contact où les limites de l'espace dans lequel la carte peut fonctionner correctement ne sont pas perceptibles.

5 Un risque supplémentaire se présente dans le cas des mémoires non volatiles de type EEPROM avec lesquelles, si l'on interrompt une opération d'écriture avant sa fin normale, il peut se faire que les données soient néanmoins écrites, et puissent donc être correctement lues peu après
10 l'écriture. Toutefois, si l'on réitère cette lecture plus tard, il n'est pas certain que l'on puisse l'effectuer correctement, car la rétention de l'information dans la cellule mémoire aura été insuffisante du fait de l'écriture interrompue avant terme.

15 Pour assurer l'intégrité des données, il est donc souhaitable que les cartes soient protégées à l'encontre de tels risques, en garantissant que les données sont soit dans l'état modifié, soit dans l'état avant demande de modification, mais jamais dans un état intermédiaire
20 indéterminé résultant d'un "arrachement".

Pour des raisons de sécurité de la transaction, il est indispensable de recommencer toute la transaction si une coupure d'alimentation vient à se produire durant le cours de la transaction, sous peine de perdre
25 irrémédiablement des données sensibles (par exemple le solde créditeur d'un porte-monnaie électronique) s'il n'est pas possible de repartir du début de la transaction.

De manière à apporter une réponse au problème énoncé ci-dessus on a songé à mémoriser l'enregistrement de
30 données dans une mémoire tampon avant de procéder à sa modification. Lorsque toutes les modifications ont été apportées aux enregistrements à modifier, les anciens enregistrements sont effacés de la mémoire tampon.

Malheureusement, cette méthode nécessite pour chaque
35 enregistrement une opération de sauvegarde dans la zone tampon, une opération d'effacement de l'enregistrement à modifier, une opération de ré-écriture et une opération

d'effacement de l'enregistrement ancien dans la zone tampon, soit 4 opérations au total. Cette opération a donc l'inconvénient de prendre beaucoup de temps ce qui représente un inconvénient majeur avec les cartes sans
5 contact.

En outre, la sauvegarde des données dans un autre emplacement de la mémoire avant d'effacer les données antérieures nécessite la présence d'un "drapeau" (flag) destiné à indiquer que l'opération de modification s'est
10 effectuée correctement ou non selon la valeur du drapeau. Le drapeau peut être un seul bit qui prend la valeur 0 ou 1 selon que la modification s'est déroulée correctement ou non. Dans la mesure où il n'est pas concevable pour des raisons évidentes d'enregistrer des bits de contrôle au
15 même emplacement que les données, la seule solution consiste à enregistrer le drapeau (le ou les bits de contrôle) dans un emplacement de mémoire réservé à cet effet et donc un bloc entier de 16 ou 32 bits alors qu'un seul bit ou quelques bits suffisent.

20 Les inconvénients cités ci-dessus prennent encore plus d'importance lorsque la carte à mémoire est utilisée dans certaines applications ne nécessitant qu'une mémoire de faible capacité où il devient impératif de ne pas gaspiller des positions de la mémoire et dans lesquelles la
25 valeur des données modifiées à chaque transaction est une fonction monotone dans le temps. Dans de telles applications, l'enregistrement de données en mémoire est soit un compteur croissant qui s'incrémente dans le temps comme par exemple une machine à photocopier, soit un
30 compteur décroissant dans le cas d'une carte pour transport en commun où la valeur de l'enregistrement est décrémentée d'une unité à chaque voyage, soit un porte-monnaie électronique où la valeur de l'enregistrement ne peut aller qu'en décroissant.

Exposé de l'invention

C'est pourquoi le but de l'invention est de réaliser un procédé de modification de données dans une carte à mémoire lors d'une transaction qui s'effectue dans un
5 minimum de temps compatible avec le temps d'accès limité à la carte durant la transaction.

Un autre but de l'invention est de réaliser un procédé de modification de données dans une carte à mémoire du type carte sans contact qui ne nécessite pas la
10 réservation de bits de contrôle (drapeau) dans un emplacement de la mémoire.

L'objet de l'invention est donc un procédé de modification des données dans un système de transaction par carte comprenant une carte à mémoire ou équivalent et un
15 lecteur apte à lire la carte lorsque celle-ci se trouve dans une position déterminée par rapport au lecteur, la carte comprenant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les
20 transactions effectuées par la carte, chaque transaction entraînant la modification de la valeur de données, cette dernière étant une fonction monotone dans le temps. A chaque transaction, une opération d'écriture de la valeur de données effectue l'écriture de la nouvelle valeur de
25 données dans un premier emplacement parmi deux emplacements prédéfinis formant un compteur dans la mémoire, l'opération d'écriture effectuant l'effacement de l'ancienne valeur de données enregistrée dans le deuxième emplacement de sorte qu'à la fin de l'opération d'écriture effectuée
30 correctement le premier emplacement contient la nouvelle valeur de donnée alors que le deuxième emplacement contient la valeur zéro.

Description brève des figures

35 Les buts, objets et caractéristiques de l'invention apparaîtront plus clairement à la lecture de la description qui suit faite en référence aux dessins dans lesquels :

- La figure 1 est une représentation schématique de la mémoire d'une carte à mémoire dans laquelle est mis en œuvre le procédé selon l'invention,
- 5 • La figure 2 est une représentation schématique du contenu du compteur à deux étages de la mémoire pour chaque phase de l'opération d'écriture,
- La figure 3 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une première situation après arrachement,
- 10 • La figure 4 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une deuxième situation après arrachement,
- 15 • La figure 5 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une troisième situation après arrachement,
- La figure 6 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une quatrième situation après arrachement, et
- 20 • La figure 7 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une cinquième situation après arrachement.
- 25

Description détaillée de l'invention

30 Dans une carte à puce du type mémoire à logique câblée utilisée dans les applications nécessitant peu de mémoire, les emplacements de mémoire sont comptés. Ainsi, la mémoire d'une telle carte à puce illustrée sur la figure 1 est une mémoire du type EEPROM ayant une capacité de 32 mots de 16 bits. L'invention décrite ci-dessous

35 permet d'éviter de disposer dans la mémoire d'une zone de contrôle obligeant à réserver un mot entier. Pour cela, deux emplacements de mémoire formant un compteur à deux

étages (étage A, étage B) sont réservés à l'enregistrement de la nouvelle valeur de données à chaque transaction effectuée entre le lecteur et la carte à mémoire.

Les principes de l'invention sont mis à profit dans
5 toutes les applications où la valeur de données modifiée à chaque transaction est une fonction monotone dans le temps. Dans certains cas (par exemple carte utilisée pour effectuer des photocopies), la valeur enregistrée est
10 incrémentée alors que dans d'autres applications telles que l'accès à des zones d'accès contrôlé ou le porte-monnaie électronique, la valeur de données va en décroissant. Cependant, il est préférable d'utiliser une incrémentation plutôt qu'une décrémentation du compteur. En effet, lorsqu'il y a arrachement, le risque est qu'il n'y ait pas
15 une rétention correcte des bites qui ont été écrits en mémoire. Dans ce cas, la valeur enregistrée peut diminuer parce que chaque bit 1 peut retomber à 0. Si on utilise une décrémentation, la valeur mal écrite allant en décroissant, sa décroissance fait courir un risque au titulaire de la
20 carte dans la mesure où il n'est pas possible de savoir si la valeur en mémoire résulte d'une décrémentation normale ou d'une décroissance anormale du contenu de la mémoire. Au contraire, lorsqu'on utilise l'incrémentation, la décroissance de la mémoire ne présente pas de risque dans
25 la mesure où la valeur à prendre en considération est la valeur précédente avant incrémentation lorsqu'il y a décroissance de la valeur mal enregistrée suite à un arrachement.

Dans le cas d'une décrémentation, il est aisé de
30 considérer à chaque fois le complément à deux en binaire de la valeur de données. Ainsi, dans ce qui suit, la valeur de données est incrémentée à chaque transaction quelle que soit l'application considérée.

Le procédé selon l'invention consiste à enregistrer
35 la nouvelle valeur de données qui a fait l'objet de la modification dans l'étage du compteur qui contenait la valeur 0 et à effacer l'autre étage du compteur pour mettre

sa valeur à 0. Ces deux phases qui ne peuvent pas être inversées, sont déclenchées par une instruction d'écriture de la nouvelle valeur provenant du lecteur au moment de la transaction.

5 La figure 2 illustre le déroulement normal des opérations. Au départ, la lecture du compteur fait apparaître la valeur X dans l'étage A et la valeur 0 dans l'étage B. L'instruction d'écriture effectue ensuite l'écriture de la nouvelle valeur Y dans l'étage B, puis
10 l'effacement de la valeur X de l'étage A. Donc, le compteur est incrémenté en une seule instruction.

Malheureusement, un arrachement de la carte peut se produire durant la transaction, en particulier lorsque la carte à puce est une carte sans contact. Dans ce cas
15 l'opération d'écriture ne se déroule pas correctement et soit l'écriture de la nouvelle valeur ne s'est pas faite correctement, soit l'ancienne valeur n'a pas été effacée. Dans ce cas, la transaction n'aboutit pas ou n'est pas validée. Ceci peut avoir comme résultat de ne pas autoriser
20 l'ouverture d'un portillon d'accès à une zone à accès contrôlée ou de ne pas permettre un achat par un terminal de commerçant dans le cas d'un porte-monnaie électronique.

Le titulaire de la carte recommence alors l'opération consistant à faire passer sa carte dans ou devant un
25 lecteur. Celui-ci effectue en premier la lecture du compteur qui fait apparaître qu'aucun des deux étages du compteur n'est à la valeur 0. Il en déduit immédiatement qu'il y a eu arrachement et procède alors à la réparation du compteur comme décrit ci-dessous.

30 Les figures 3 à 7 illustrent les opérations de réparation du compteur lorsqu'il y a eu arrachement selon que cet arrachement s'est produit pendant la phase d'écriture, entre la phase d'écriture et la phase d'effacement ou pendant la phase d'effacement.

35 Dans une première situation illustrée par la figure 3, l'arrachement a eu lieu pendant la phase d'écriture, la valeur Y a été écrite mais la valeur X n'a pas été effacée.

Dans ce cas, et bien que la valeur Y soit correcte, il n'est pas possible de garantir la rétention de cette valeur dans l'étage B. La valeur Y est donc ré-écrite avant de procéder à l'effacement de la valeur X de l'étage A pour la
5 mettre à 0. A noter que l'écriture d'un emplacement de mémoire est une fonction OU entre la valeur qui s'y trouve et la nouvelle valeur et que par conséquent, on ne peut qu'écrire une nouvelle valeur que si l'ancienne valeur est égale à 0 ou à identiquement la nouvelle valeur (ce qui est
10 le cas ici).

Dans une deuxième situation illustrée sur la figure 4, l'arrachement a eu lieu pendant la phase d'écriture, une valeur Y' comprise entre X et Y a été écrite dans l'étage B et la valeur X n'a pas été effacée de l'étage A. Dans ce
15 cas, une première opération d'écriture procède à la ré-écriture de Y' dans l'étage B et à l'effacement de X de l'étage A. Puis une opération d'écriture procède à l'écriture de Y dans l'étage A et à l'effacement de Y' de l'étage B, de sorte que le compteur se retrouve dans une
20 situation normale où un étage contient la nouvelle valeur et où l'autre étage est à 0.

Dans une troisième situation illustrée sur la figure 5, l'arrachement a eu lieu pendant la phase d'écriture, une valeur Y' inférieure à X a été écrite dans l'étage B et la
25 valeur X n'a pas été effacée. Dans ce cas, une première opération de ré-écriture procède à la ré-écriture de la valeur X dans l'étage A et à l'effacement de Y' de l'étage B. Ceci se justifie par le fait que la réparation du compteur s'effectue toujours avec la valeur la plus grande qui est, en l'occurrence, la valeur X. Puis une opération
30 d'écriture procède à l'écriture de la valeur Y dans l'étage B et à l'effacement de X de l'étage A.

Dans une quatrième situation illustrée sur la figure 6, l'arrachement a eu lieu entre la phase d'écriture et la
35 phase d'effacement, la valeur Y a été enregistrée dans l'étage B mais la valeur X n'a pas été effacée de l'étage A. Comme on ne peut pas garantir la rétention de la valeur

Y, une opération de ré-écriture procède à la ré-écriture de la valeur Y dans l'étage B et à l'effacement de la valeur X de l'étage A.

5 Dans une cinquième situation illustrée sur la figure 7, l'arrachement a eu lieu pendant la phase d'effacement, la valeur Y a été écrite dans l'étage B mais la valeur X n'a pas été effacée correctement et une valeur X' se trouve dans l'étage A. Il faut donc procéder à une opération de ré-écriture de la valeur Y dans l'étage B qui permet alors
10 l'effacement de la valeur X' de l'étage A.

Dans toutes les situations qui viennent d'être décrites, la réparation du compteur a été entreprise parce qu'aucun des deux étages ne contenait la valeur 0, et après réparation, l'un des deux étages contient la nouvelle
15 valeur de données alors que l'autre étage contient 0. A noter que, dans aucune des situations, le compteur se retrouve dans un état où la valeur maximale se trouvant dans l'étage A ou dans l'étage B est inférieure à l'ancienne valeur (X).

REVENDICATIONS

1. Procédé de modification des données dans un système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte comprenant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, chaque transaction entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps,

ledit procédé étant caractérisé en ce que, à chaque transaction, une opération d'écriture de ladite valeur de données effectue l'écriture de la nouvelle valeur de données (Y) dans un premier emplacement (B) parmi deux emplacements prédéfinis formant un compteur dans ladite mémoire, ladite opération d'écriture effectuant l'effacement de l'ancienne valeur de données (X) enregistrée dans le deuxième emplacement (A) desdits deux emplacements de sorte qu'à la fin de l'opération d'écriture effectuée correctement ledit premier emplacement contient ladite nouvelle valeur de donnée alors que ledit deuxième emplacement contient la valeur zéro.

2. Procédé selon la revendication 1, dans lequel la valeur de données enregistrée dans un desdits deux emplacements (A ou B) est incrémentée à chaque opération d'écriture.

3. Procédé selon la revendication 2, dans laquelle la transaction n'est pas validée du fait que ladite opération d'écriture ne s'est pas effectuée correctement à cause d'un arrachement de ladite carte

au cours de la transaction, aucun des deux étages dudit compteur n'ayant enregistré une valeur égale à zéro.

4. Procédé selon la revendication 2, comprenant en outre
5 une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu pendant la phase
10 d'écriture de ladite nouvelle valeur.
5. Procédé selon la revendication 2, comprenant en outre,
lorsque ledit premier emplacement (B) contient une
valeur incorrecte (Y') comprise entre ladite ancienne
15 valeur de donnée (X) et ladite nouvelle valeur de données (Y), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite valeur incorrecte dans ledit premier emplacement et à effacer ladite ancienne valeur dudit deuxième
20 emplacement, suivie d'une opération d'écriture consistant à écrire ladite nouvelle valeur dans ledit deuxième emplacement (A) et à effacer ladite valeur incorrecte dudit premier emplacement.
- 25 6. Procédé selon la revendication 2, comprenant en outre,
lorsque ledit premier emplacement (B) contient une valeur de données incorrecte (Y') inférieure à ladite ancienne valeur (X), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire
30 ladite ancienne valeur de données (X) dans ledit deuxième emplacement (A) et à effacer ladite valeur de données incorrecte, suivie d'une opération d'écriture, consistant à écrire ladite nouvelle valeur de données (y) dans ledit premier emplacement et à effacer ladite
35 ancienne valeur de données dudit deuxième emplacement.

7. Procédé selon la revendication 2, comprenant en outre une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur de données (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu entre la phase d'écriture de ladite nouvelle valeur de données et la phase d'effacement de ladite ancienne valeur de données.

8. Procédé selon la revendication 2, comprenant en outre, lorsque l'arrachement a eu lieu pendant la phase d'effacement de ladite ancienne valeur de données (X) et qu'une valeur de données incorrecte (X') est enregistrée dans ledit deuxième emplacement (A), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite valeur de données incorrecte dudit deuxième emplacement.

9. Système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte incluant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, chaque transaction entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps ;

ledit système étant caractérisé en ce que ladite mémoire comprend un premier emplacement et un deuxième emplacement prédéfinis formant un compteur, chaque transaction donnant lieu à une instruction d'écriture effectuant l'écriture d'une nouvelle valeur de données

(Y) dans ledit premier emplacement (B) et l'effacement de l'ancienne valeur de données (X) dudit deuxième emplacement (A), de sorte qu'à la fin de l'opération d'écriture ledit premier emplacement contient ladite
5 nouvelle valeur de données alors que ledit deuxièmement emplacement contient la valeur zéro.

10. Système selon la revendication 9, dans lequel ladite carte à mémoire est une carte sans contact.

ADRESSE	SEIZE BITS PAR MOT
0	NUMERO DE SERIE
1	
2	
3	
4	
5	ZONE 1
6	
7	
8	
9	
10	ZONE 2
11	
12	
13	
14	
15	
16	
17	
18	COMPTEUR ETAGE A
19	COMPTEUR ETAGE B
20	ZONE 3
21	
22	
23	
24	
25	
26	
27	
28	ZONE 4
29	
30	
31	

FIG. 1

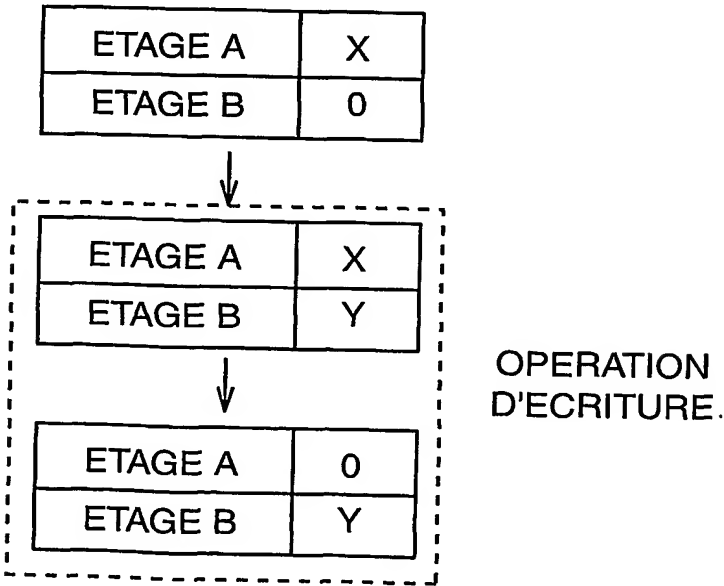


FIG. 2

2/4

ETAGE A	X
ETAGE B	Y



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 3

ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	Y'



ETAGE A	0
ETAGE B	Y'

OPERATION
DE RE-ECRITURE



ETAGE A	Y
ETAGE B	Y'



ETAGE A	Y
ETAGE B	0

OPERATION
D'ECRITURE

FIG. 4

3/4

ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	0

OPERATION
DE RE-ECRITURE



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
D'ECRITURE

FIG. 5

ETAGE A	X
ETAGE B	Y



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 6

4/4

ETAGE A	X'
ETAGE B	Y



ETAGE A	X'
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 7